

In the Claims:

Please amend Claims 1 and 7, cancel Claims 10-20 and add new Claims 21-31, all as shown below. Applicant reserves the right to prosecute any originally presented or withdrawn claims in a future or continuing application.

1. (Currently Amended) A system for maintaining security in a distributed computing environment, comprising:

(1) a policy manager, coupled to a network, including  
a database for storing a security policy including a plurality of rules; and  
a policy distributor, coupled to the database, for distributing the plurality of rules through the network;

(2) a security engine located on a client coupled to the network, for storing a set of the plurality of rules constituting a local customized security policy received through the network from the policy distributor, and for enforcing the local customized security policy with respect to an application at the client; and

(3) an application, coupled to the security engine;  
wherein the security policy is updated by keeping track of a series of incremental changes to the security policy, computing an accumulated delta that reflects the series of incremental changes and sending the accumulated delta to the security engine from the policy manager such that the security engine uses the delta to update the local customized security policy.

2. (Previously Presented) The system of claim 1, wherein the rules are stored separate from the application rather than being embedded in the application.

3. (Previously Presented) The system of claim 1, wherein the security engine further comprises:

an engine for evaluating a request to access the application based on the set of the plurality of rules; and

an application programming interface (API) for enabling the application and the engine to communicate.

4. (Original) The system of claim 3, wherein the security engine further comprises: a plug-in

application programming interface (API) for extending capabilities of the security engine.

5. (Original) The system of claim 1, further comprising: location means for enabling components in the system to locate each other through the network.

6. (Original) The system of claim 1, wherein the policy manager and the policy distributor are hosted on a first server, the security engine and the application are hosted on a second server, and the first and second servers are communicatively coupled to each other through the network.

7. (Currently Amended) A system for maintaining security for an application in a distributed computing environment, comprising:

an engine located at a client coupled to a network, for storing a set of rules constituting a local customized policy received through the network from a centralized location, and for enforcing the local customized policy at an application level of the client;

an interface coupled to the engine for evaluating the local customized policy in order to control access to an application at the client; and

an application, coupled to the interface so as to communicate with the engine;  
wherein the local customized policy is updated by keeping track of incremental changes to the policy, computing an accumulated delta that reflects all the incremental changes and sending the accumulated delta to the engine from the centralized location such that the engine uses the delta to update the local customized policy.

8. (Previously Presented) The system of claim 7, wherein the engine stores the rules separate from the application rather than being embedded in the application.

9. (Original) The system of claim 7, further comprising: a plug-in application programming interface (plug-in API) for extending capabilities of the security engine.

10-20. (Canceled)

21. (New) A method for maintaining security in a distributed computing environment, comprising:

maintaining a policy manager coupled to a network, including a database for storing a security policy and a policy distributor, coupled to the database, for distributing a portion of the security policy through the network;

maintaining a security engine located on a client coupled to the network, for storing a local customized security policy received through the network from the policy distributor, and for enforcing the local customized security policy with respect to an application at the client; and

maintaining an application, coupled to the security engine;

receiving a series of incremental changes to the security policy at the policy manager;

computing an accumulated delta that reflects the series of incremental changes to the security policy; and

distributing the accumulated delta to the security engine on the client wherein the security engine uses the delta to update the local customized security policy.

22. (New) The method of claim 21, further comprising:

storing the accumulated delta in a policy change tracking table before distributing it to the security engine.

23. (New) The method of claim 22, further comprising:

reconstructing an updated local customized security policy back to a previously distributed version by using the accumulated delta stored in the policy change tracking table.

24. (New) The method of claim 21 wherein the security policy includes a plurality of rules for controlling access to securable objects.

25. (New) The method of claim 24 wherein the series of incremental changes include at least one or more of adding a rule, deleting a rule and amending a rule.

26. (New) A method for maintaining security in a distributed computing environment, comprising:

maintaining an engine at a client coupled to a network, the engine adapted to store a set of rules constituting a local customized policy received through the network from a centralized location, and for enforcing the local customized policy at an application level of the client;

maintaining an interface coupled to the engine for evaluating the local customized policy in order to control access to securable components; and

maintaining an application, coupled to the interface so as to communicate with the engine; receiving a series of incremental changes to the set of rules at the centralized location; computing an accumulated delta to reflect the series of incremental changes; and communicating the accumulated delta to the engine at the client such that the engine employs the accumulated delta to update the local customized policy.

27. (New) The method of claim 26, further comprising:

storing the accumulated delta in a policy change tracking table before distributing it to the engine.

28. (New) The method of claim 27, further comprising:

reconstructing an updated local customized policy back to a previously distributed version by employing the accumulated delta stored in the policy change tracking table.

29. (New) The method of claim 26 wherein the series of incremental changes include at least one or more of adding a rule, deleting a rule and amending a rule.

30. (New) A computer readable medium having instructions stored thereon which when executed by one or more processors cause a system to:

maintain a policy manager coupled to a network, including a database for storing a security policy and a policy distributor, coupled to the database, for distributing a portion of the security policy through the network;

maintain a security engine located on a client coupled to the network, for storing a local customized security policy received through the network from the policy distributor, and for enforcing the local customized security policy with respect to an application at the client; and

maintain an application, coupled to the security engine;  
receive a series of incremental changes to the security policy at the policy manager;  
compute an accumulated delta that reflects the series of incremental changes to the security policy; and  
distribute the accumulated delta to the security engine on the client wherein the security

engine uses the delta to update the local customized security policy.

31. (New) A computer readable medium having instructions stored thereon which when executed by one or more processors cause a system to:

maintain an engine at a client coupled to a network, the engine adapted to store a set of rules constituting a local customized policy received through the network from a centralized location, and for enforcing the local customized policy at an application level of the client;

maintain an interface coupled to the engine for evaluating the local customized policy in order to control access to securable components; and

maintain an application, coupled to the interface so as to communicate with the engine; receive a series of incremental changes to the set of rules at the centralized location; compute an accumulated delta to reflect the series of incremental changes; and communicate the accumulated delta to the engine at the client such that the engine employs the accumulated delta to update the local customized policy.